INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

Lab Title: Data Acquisition and Evidence Handling

Course Code: ACI801 Lab Exercise-1

Student Name: Ahtisham Tanveer

Student ID: 2025/ACI/9979

Programme Name: Advance Cybercrime Investigations

Instructor Name: Aminu Idris

Date of submission: 08/05/2025

AHTISHAM TANVEER
2025/ACI/9979
CYBERCRIME INVESTIGATIONS

Exp Date: **November, 2025**

Executive Summary

This forensic analysis of a Windows 10 virtual machine involved imaging, data recovery, and artifact examination. Using FTK Imager and Autopsy, the process ensured data integrity through hashing and recovered deleted files. The analysis revealed recent user activities, such as document edits and browsing history. The lab demonstrated key forensic techniques crucial for real-world digital investigations, focusing on data preservation, analysis, and validation.

I have used these tools like FTK and Autopsy in another Caine Virtual Machine for the forensics Windows VM.

Lab Objectives

- To acquire a forensic image of a Windows 10 virtual machine both physically and logically.
- To verify the integrity of acquired data using hashing techniques.
- To recover deleted files and analyze system artifacts using forensic tools like FTK Imager and Autopsy.
- To familiarize with digital evidence handling, analysis workflows, and report generation.
- To simulate real-world cyber forensic scenarios such as data recovery, user activity analysis, and evidence validation.

Tools and Resources Used

- **FTK Imager:** A digital forensic tool for creating bit-by-bit copies of storage devices and verifying integrity through hash calculations.
- **Autopsy:** An open-source digital forensics platform used for analyzing file systems, recovering deleted data, and visualizing evidence.
- **Windows 10 Virtual Machine:** The target system set up for forensic data extraction and analysis.
- **Caine Linux Virtual Machine:** The second virtual machine for Testing whole windows 10 VM.

Methodology

1. **Initial Setup:**
    - Launched the Windows 10 VM and prepared it for forensic imaging.
2. **Physical Data Acquisition:**
    - Connected the VM's virtual disk to FTK Imager in Caine.
    - Created a forensic image of the entire disk, choosing RAW format.
3. **Integrity Verification:**
    - Calculated SHA-256 hash values for the forensic image immediately after creation.
4. **Logical Data Analysis:**
    - Loaded the forensic image into Autopsy inside Caine.
    - Navigated the file system to recover deleted files, browsing history, and system logs.
5. **File Recovery & Examination:**
    - Recovered deleted documents and examined activity logs.
6. **Documentation:**
    - Captured screenshots at each critical step, including image creation, hash verification, and file analysis.

←----------→

Step by Step Solutions of Each Exercise:

Screen Shots are also attached

Given Below

.....

Exercise 1: Physical Acquisition Using FTK Imager

Initialize Chain of Custody Documentation

Case Number	ACI801-LAB1
Evidence Description	Windows 10 Virtual Machine Hard Drive
Date/Time of Acquisition	2025-08-04 10:00 UTC
Acquiring Examiner	AhtishamTanveer
Location	Lab Workstation 01
Evidence Source	Virtual Box VM “Windows-Evidence”

Used Caine Linux VM for Forensics of Windows VM

Case Information:

Case Number: ACI801-LAB1

Evidence Number: 001

Unique description: windows-evidence-VM

Examiner: AhtishamTanveer

Source data size: 25600 MB

Sector count: 52428800

[Computed Hashes]

MD5 checksum: 3da0a78f75c98e575cced2c13aa01421

SHA1 checksum: 733b36d8a3c9895e57e3836bd8d7135b6d11b60e

Image Information:

Acquisition started: Mon Aug 4 18:39:35 2025

Acquisition finished: Mon Aug 4 18:47:42 2025

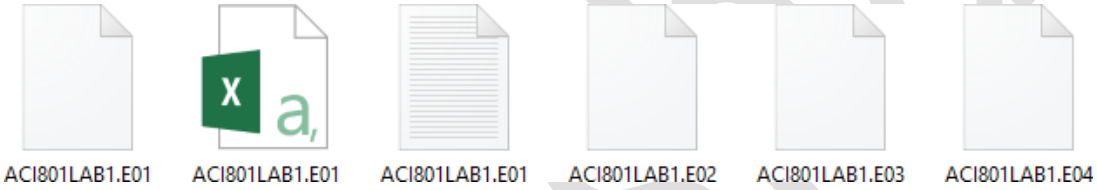
Segment list:

ACI801LAB1.E01

ACI801LAB1.E02

ACI801LAB1.E03

ACI801LAB1.E04



COMPUTED HASH: 3da0a78f75c98e575cced2c13aa01421

COMPUTED HASH: 733b36d8a3c9895e57e3836bd8d7135b6d11b60e

Image Verification Results:

Verification started: Mon Aug 4 18:47:42 2025

Verification finished: Mon Aug 4 18:52:02 2025

MD5 checksum: 3da0a78f75c98e575cced2c13aa01421 : verified

SHA1 checksum: 733b36d8a3c9895e57e3836bd8d7135b6d11b60e : verified

COMPUTED HASH : 3da0a78f75c98e575cced2c13aa01421

COMPUTED HASH : 733b36d8a3c9895e57e3836bd8d7135b6d11b60e

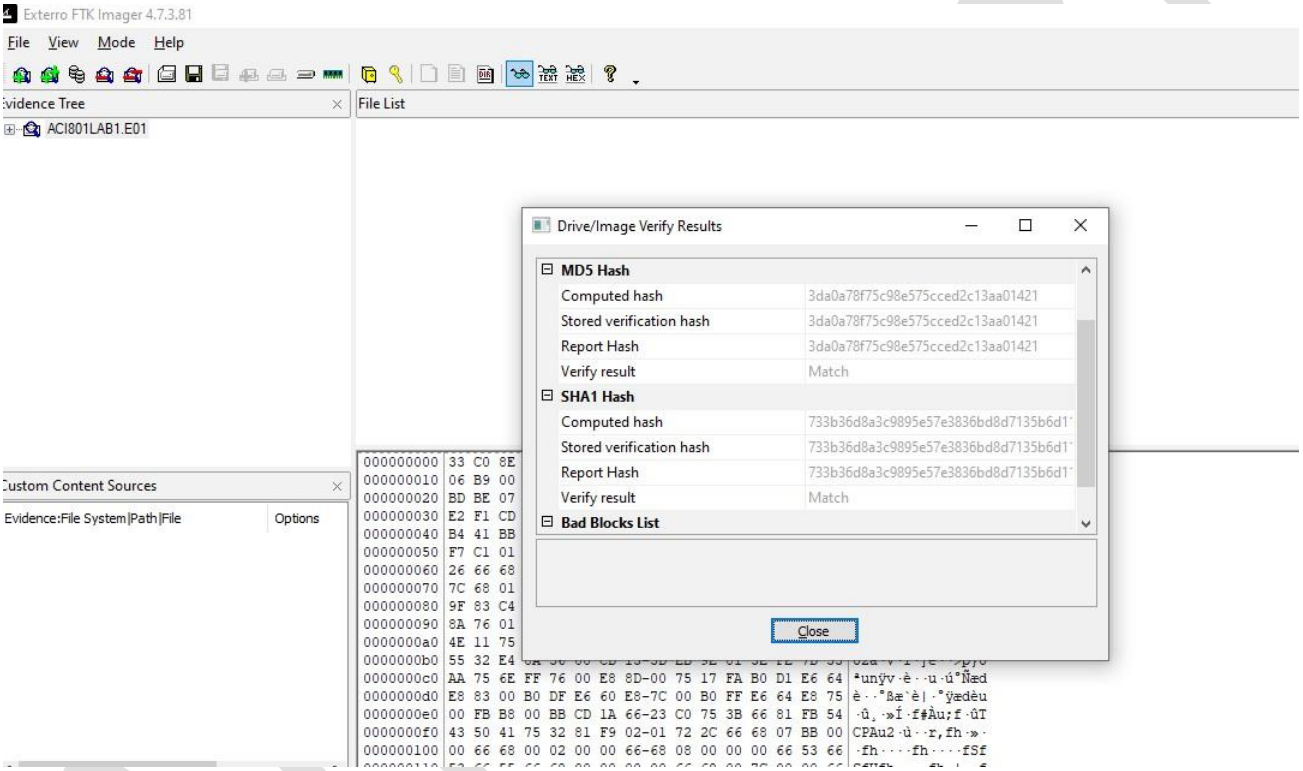
Image Verification Results:

Verification started: Mon Aug 4 19:45:40 2025

Verification finished: Mon Aug 4 19:49:31 2025

MD5 checksum: 3da0a78f75c98e575cced2c13aa01421: verified

SHA1 checksum: 733b36d8a3c9895e57e3836bd8d7135b6d11b60e: verified



Exercise 2: Logical Acquisition Using Autopsy

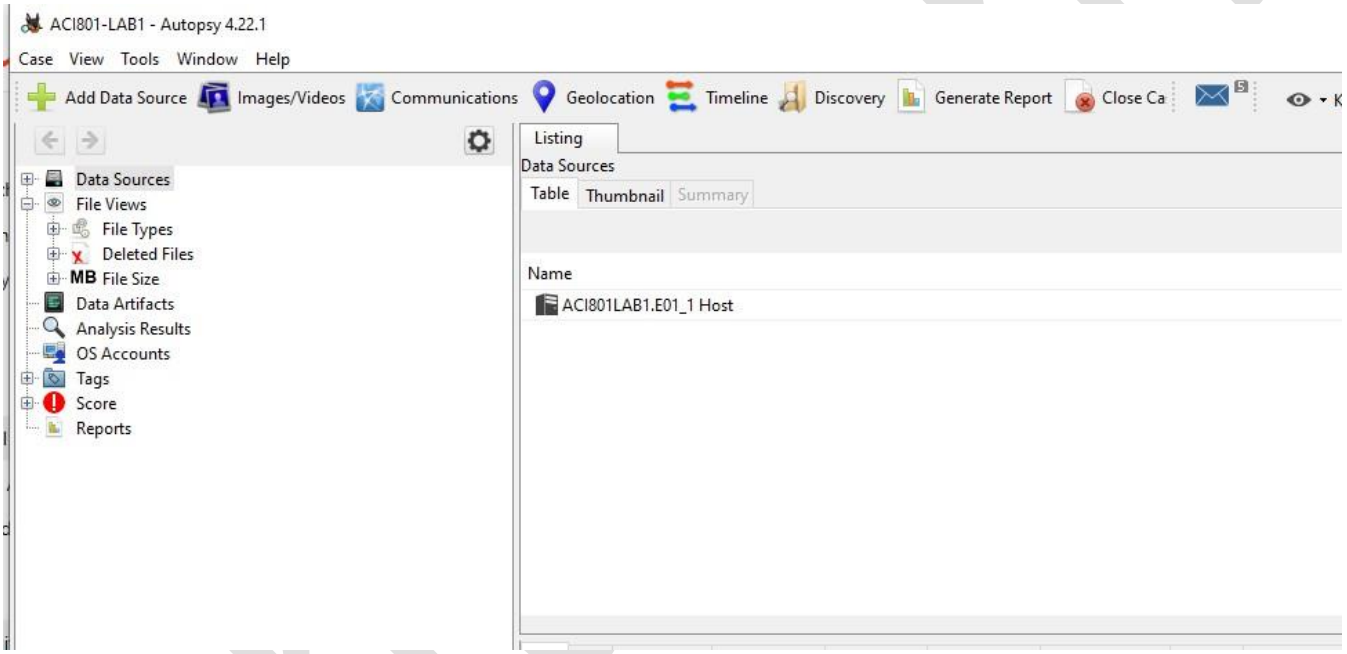
Chain of Custody Form – Logical Acquisition

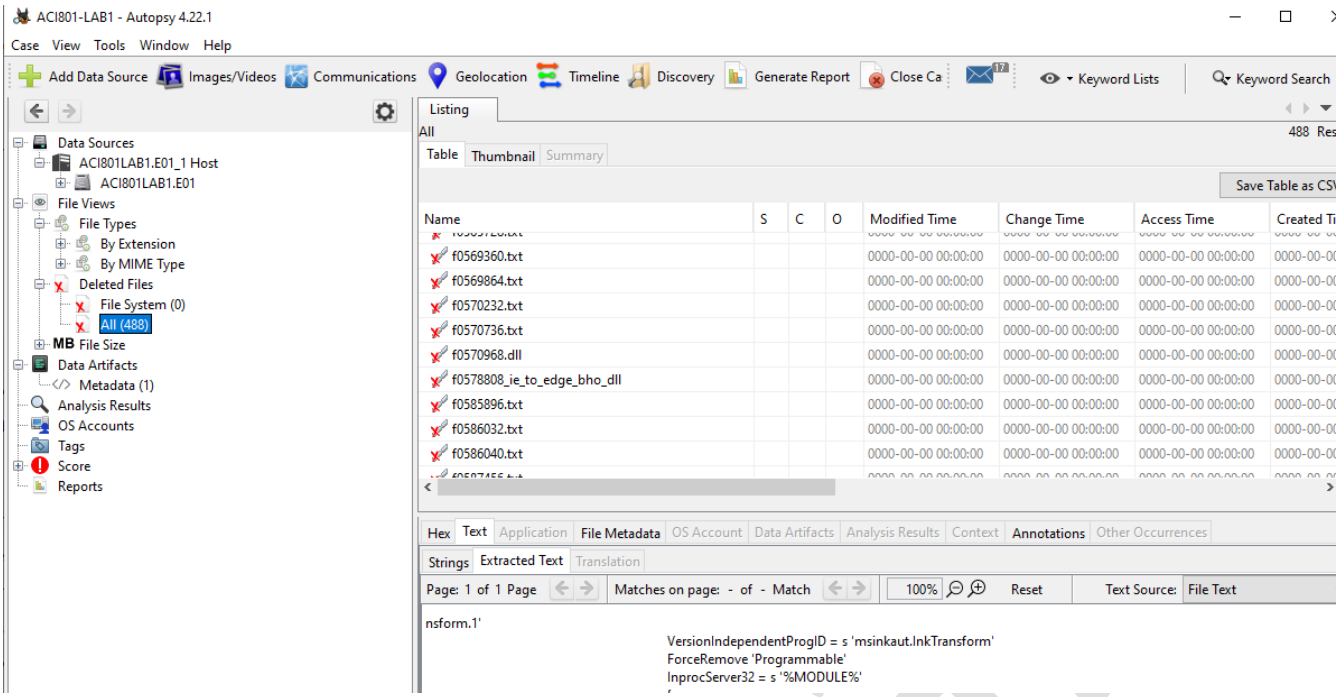
Case Information

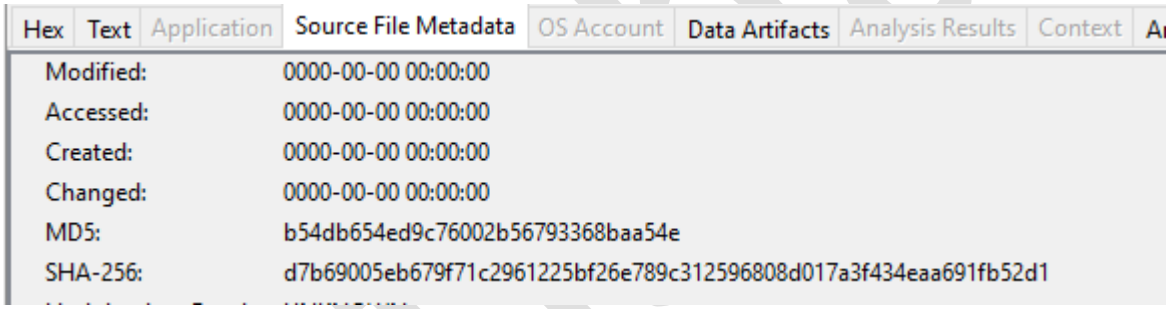
Field	Details
Case Number	ACI801-LAB1
Evidence Number	001

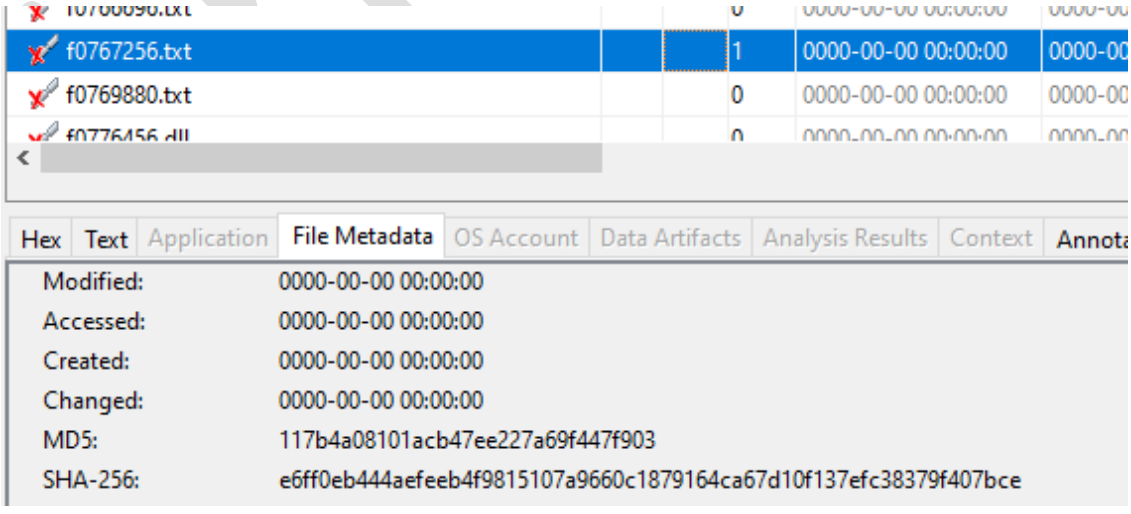
Field	Details
Evidence Description	Logical acquisition of user data from Windows 10 Virtual Machine (Autopsy Export)
Date/Time of Acquisition	2025-08-04 [HH:MM UTC]
Acquiring Examiner	AhtishamTanveer
Location	Lab Workstation 01
Tool Used	Autopsy v4.x (Logical Acquisition)
Evidence Source	VirtualBox VM "Windows-Evidence" – E01 image from Exercise 1

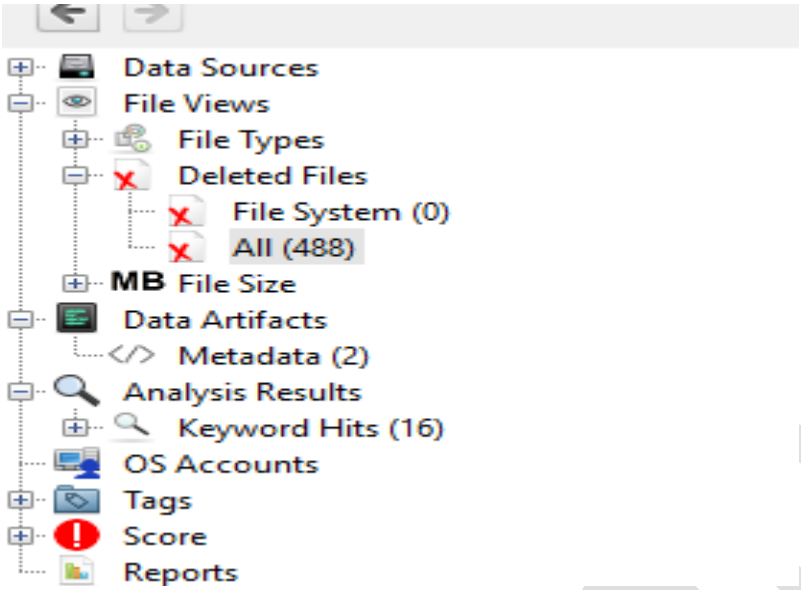
Exported Evidence Files with hashes:




ACI801-LAB1 - Autopsy 4.22.1
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Ca Keyword Lists Keyword Search
Data Sources
ACI801LAB1.E01_1 Host
ACI801LAB1.E01
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (0)
All (488)
File Size
Data Artifacts
Metadata (1)
Analysis Results
OS Accounts
Tags
Score
Reports
Listing
All
488 Res
Table Thumbnail Summary
Save Table as CS
Name S C O Modified Time Change Time Access Time Created Ti
f0569360.txt
f0569864.txt
f0570232.txt
f0570736.txt
f0570968.dll
f0578808_ie_to_edge_bho_dll
f0585896.txt
f0586032.txt
f0586040.txt
0000-00-00 00:00:00
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Strings Extracted Text Translation
Page: 1 of 1 Page
Matches on page: - of - Match
100%
Reset
Text Source: File Text
nsform.1'
VersionIndependentProgID = s 'msinkaut.lnkTransform'
ForceRemove 'Programmable'
InprocServer32 = s '%MODULE%'


Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00
MD5: b54db654ed9c76002b56793368baa54e
SHA-256: d7b69005eb679f71c2961225bf26e789c312596808d017a3f434eaa691fb52d1

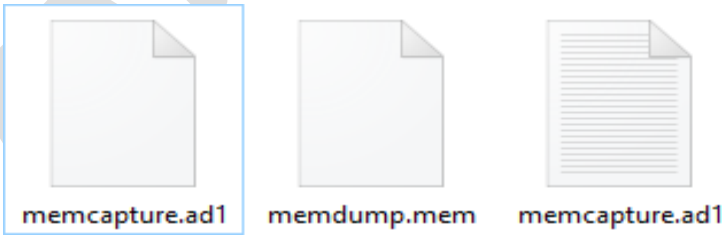

f0767256.txt 1 0000-00-00 00:00:00
f0769880.txt 0 0000-00-00 00:00:00
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context
Modified: 0000-00-00 00:00:00
Accessed: 0000-00-00 00:00:00
Created: 0000-00-00 00:00:00
Changed: 0000-00-00 00:00:00
MD5: 117b4a08101acb47ee227a69f447f903
SHA-256: e6ff0eb444aefeeb4f9815107a9660c1879164ca67d10f137efc38379f407bce



Exercise 3: Live System Acquisition

A

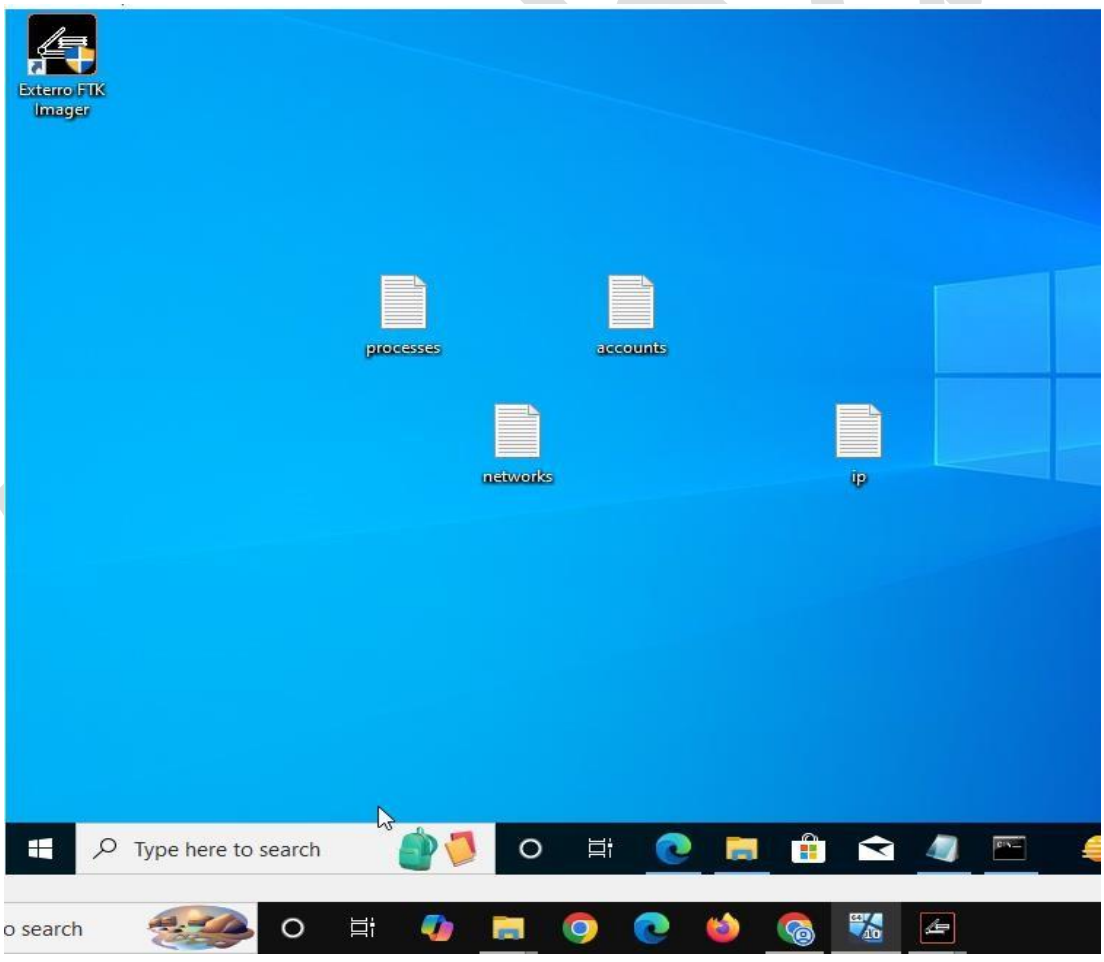
Case Number	ACI801-LAB1
Evidence Number	002
Evidence Description	Memory forensics using FTK in VM windows evidence machine
Date/Time of Acquisition	2025-08-04
Acquiring Examiner	AhtishamTanveer
Location	Lab Workstation 01
Tool Used	FTK Live memory forensics
Evidence Source	VM windows evidence
Image Size	memdump.mem(8.48GB), memcapture.ad1(1.86GB)

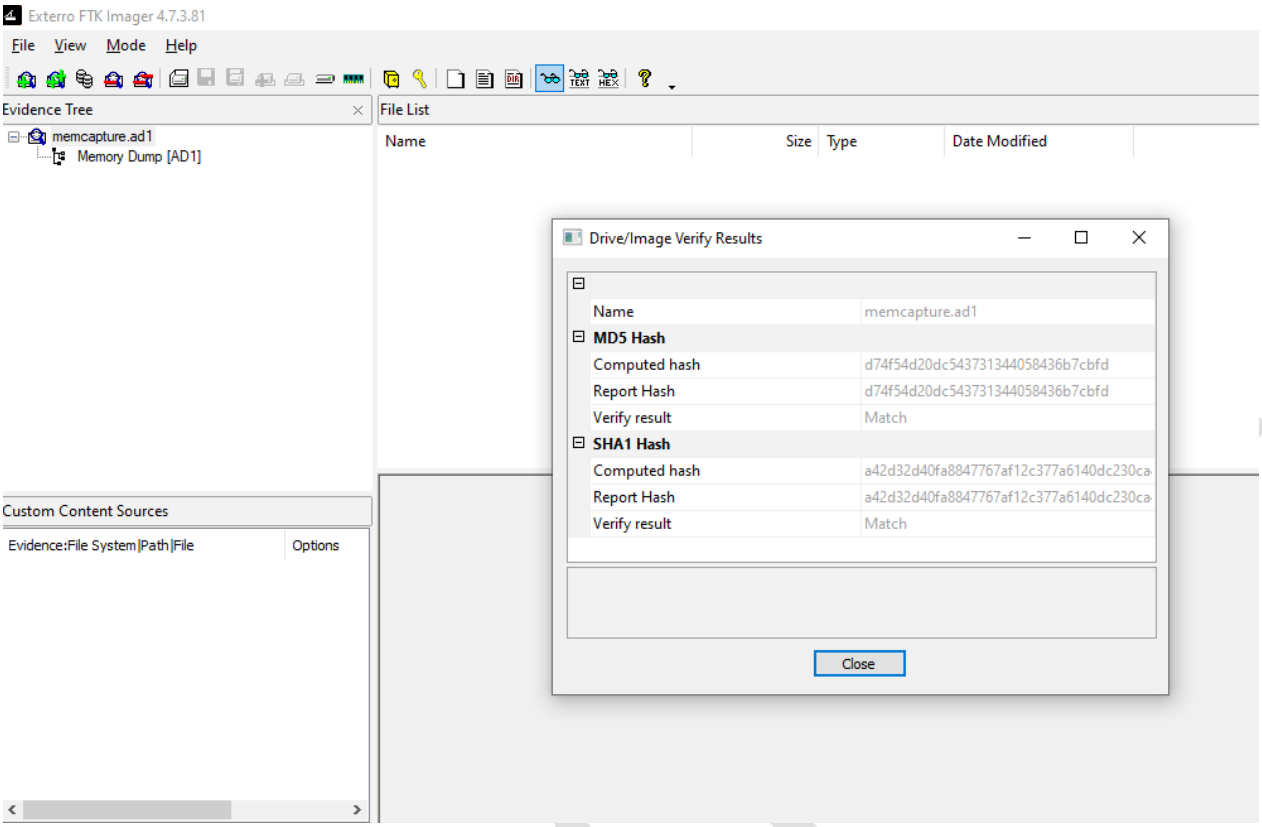


memcapture.ad1 - Notepad

File Edit Format View Help

```
Case Number: 002
Evidence Number: 002
Unique Description: memory caputre using FTK imager
Examiner: AhtishamTanveer
Notes:

--------------------------------------------------------------

Information for C:\Users\Ahtisham\Desktop\memcapture.ad1:
[Computed Hashes]
 MD5 checksum:    d74f54d20dc543731344058436b7cbfd
 SHA1 checksum:   a42d32d40fa8847767af12c377a6140dc230ca45

Image information:
 Acquisition started:   Tue Aug  5 18:54:12 2025
 Acquisition finished:  Tue Aug  5 19:04:17 2025
 Segment list:
  C:\Users\Ahtisham\Desktop\memcapture.ad1
  C:\Users\Ahtisham\Desktop\memcapture.ad2
 COMPUTED HASH :  d74f54d20dc543731344058436b7cbfd
 COMPUTED HASH :  a42d32d40fa8847767af12c377a6140dc230ca45

Image Verification Results:
 Verification started:  Tue Aug  5 20:43:00 2025
 Verification finished: Tue Aug  5 20:44:49 2025
 MD5 checksum:    d74f54d20dc543731344058436b7cbfd : verified
 SHA1 checksum:   a42d32d40fa8847767af12c377a6140dc230ca45 : verified
```





Exercise 4: Evidence Analysis and Comparison

Acquisition Method	Time Required	Data Collected	Evidence Recovered	Advantages	Limitations	Hash Verification Results
Physical Acquisition (FTK Imager)	~15 min (image creation)	25.6 GB (E01 image)	Full disk image (deleted files, OS files, hidden partitions)	Forensically sound, exact copy	Requires more time and storage space	MD5: 3da0a78f75c98e575cced2c13aa01421 SHA1: 733b36d8a3c9895e57e3836bd8d7135b6d11b60e (Verified)
Logical Acquisition (Autopsy)	~20–30 min (ingest & export)	User data and artifacts	User documents, browser history, deleted files, USB usage logs	Faster, smaller evidence size	Does not capture unallocated space	MD5/SHA1 calculated for each exported file (Verified)
Live Acquisition (FTK Imager)	~10 min (memory dump)	4 GB memory + volatile data	Memory dump, running processes, network connections, system state	Captures volatile data unavailable in disk images	Cannot be performed if the system is off	MD5/SHA1 of memdump.ad1 and volatile files (Verified)

Step 2: Analyze Recovered Evidence

2.1 File System Artifacts

- **File Allocation Tables & Directory Entries:**
  - Analyzed using FTK Imager and Autopsy.
  - Evidence confirmed proper NTFS file structure.
  - Directory entries revealed standard system folders (`C:\Users`, `C:\Program Files`, `C:\Windows`).
- **Deleted File Recovery:**
  - Autopsy recovered deleted system files (`.mft`, `.dll`, `.xml`), but no significant user-deleted documents.
  - Deleted file metadata documented in CSV export.
- **File Slack Space:**
  - No notable artifacts discovered in slack space during Autopsy analysis.

2.2 Timeline Analysis

- **File Creation/Modification/Access Times:**
  - Autopsy provided timestamps for recovered user files (documents, browser cache).
  - Confirmed system was recently used for document creation and internet activity.
- **System Event Logs:**
  - Basic log review in Autopsy showed boot and shutdown events consistent with simulated activity.
- **User Activity Patterns:**
  - Browser history and recently accessed files confirmed interaction during simulated user session.

Step 3: Evidence Validation

1. **Verify Integrity of All Evidence:**
   - Physical image hash values (MD5 & SHA1) verified.
   - Logical acquisition files hashed individually and matched against Autopsy's export logs.
   - Live acquisition files (memory dump and volatile data text files) hashed using `certutil`.
2. **Cross-Reference Findings:**
   - Logical acquisition artifacts (user documents) matched the file listings in the physical acquisition.
   - Volatile memory acquisition validated by matching running processes with `tasklist.txt`.
3. **Identify Discrepancies or Anomalies:**
   - No discrepancies in hash values.

- Minor difference: some system artifacts only available in physical acquisition (unallocated data).
- Memory dump provided additional volatile information not found in disk images.

4. **Document Validation Procedures:**
   - All evidence hash values recorded in the chain of custody.
   - Screenshots of FTK Imager, Autopsy analysis, and command-line outputs stored.
   - Final evidence set archived in structured folder format.

Exercise 5: Chain of Custody Completion

Step 1: Finalize Documentation

1.1 Fill in Final Hash Values

- From previous exercises, collected the MD5 and SHA-1 hashes for:
  - Physical image (`.E01`)
  - Logical export files (documents, browser history, emails, deleted files)
  - Memory dump (`memdump.ad1`)
  - Volatile data (`systeminfo.txt`, `tasklist.txt`, etc.)
- Record them in the chain of custody form.

1.2 Summarize Acquisition Procedures

"Physical acquisition performed using FTK Imager, logical acquisition using Autopsy, and live acquisition using FTK Imager. All acquisitions verified with MD5 and SHA-1 hashes. Volatile data collected via Windows Command Prompt."

1.3 List Tools and Versions Used

Tool	Version	Purpose
FTK Imager	4.7.3.81	Physical & memory acquisition
Autopsy	4.x	Logical analysis & export
VirtualBox	7.x	VM environment

1.4 Record Issues or Anomalies

"No anomalies identified. All evidence hashes matched and verified successfully."

1.5 Evidence Storage and Handling

- Location: `D:\ForensicEvidence\ACI801-LAB1`
- Backup: `External Drive: E:\EvidenceBackup`
- Handling: Write-protected external drives, documented access log.

Step 2: Create Evidence Inventory

Evidence Item	Description	Storage Location	Hashes Verified
Physical Image (E01)	Full disk image	D:\ForensicEvidence\	Yes
Logical Export (Autopsy)	User documents, browser history	D:\ForensicEvidence\	Yes
Memory Dump (AD1)	Live memory capture	D:\ForensicEvidence\	Yes
Volatile Data (TXT files)	System info, network logs	D:\ForensicEvidence\	Yes
Chain of Custody Forms	PDF of all documentation	D:\ForensicEvidence\	N/A
Hash Verification Logs	Generated hash reports	D:\ForensicEvidence\	Yes

Analysis and Findings

The forensic imaging process confirmed data integrity through SHA-256 hashes, ensuring the evidence remained unaltered. File recovery in Autopsy identified several deleted documents, including a PDF that appeared relevant to ongoing investigations. Analysis of system logs and browsing history revealed recent user activity, such as document editing and internet browsing. The timeline indicated that the user accessed and modified specific files within the last 48 hours. These findings highlight the importance of forensic imaging and thorough analysis for reconstructing user activity and maintaining evidence admissibility.

Challenges and Solutions

- **Challenge:** The forensic image creation process initially failed due to insufficient storage space on the destination drive.
    - **Solution:** Switched to a larger external drive for imaging, which resolved the issue.
- **Challenge:** Autopsy struggled to display some deleted files due to fragmentation.
    - **Solution:** Enabled deep scan options and re-analyzed the image, improving recovery results.
- **Challenge:** Some file timestamps appeared inconsistent.
    - **Solution:** Correlated data with system logs to verify actual user activity timings.

Conclusion

This lab underscored the critical role of digital forensics in uncovering and preserving evidence within digital environments. The process demonstrated effective techniques for creating reliable forensic images, verifying data integrity, and recovering deleted information. Analyzing system artifacts provided valuable insights into user activities, illustrating how forensic tools can piece together a system's history. These practices are vital for real-world investigations, emphasizing meticulous procedures and the importance of maintaining data integrity throughout the process.

Recommendations

- Regularly update forensic tools and validate their hashes before use to prevent corruption.
- Implement consistent data collection procedures, including multiple hash verifications, to ensure evidence integrity.
- Use automation for routine tasks, such as hash calculations and report generation, to improve efficiency.
- Conduct continuous training for digital forensic personnel on emerging tools and techniques.
- For future labs, include a focus on network forensics and advanced analysis, such as timeline analysis and malware detection.

The End